(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 April 2005 (14.04.2005)

PCT

(10) International Publication Number
WO 2005/033914 A1

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/IB2004/051976

(22) International Filing Date: 5 October 2004 (05.10.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
03103686.6 6 October 2003 (06.10.2003) EP

(71) Applicant *(for all designated States except US)*: **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **HASELSTEINER, Ernst** [AT/AT]; Triester Strasse 64, A-1101 Vienna (AT). **SUENG, Gregor** [AT/AT]; Triester Strasse 64, A-1101 Vienna (AT). **STEINER, Ernst** [AT/AT]; Triester Strasse 64, A-1101 Vienna (AT).

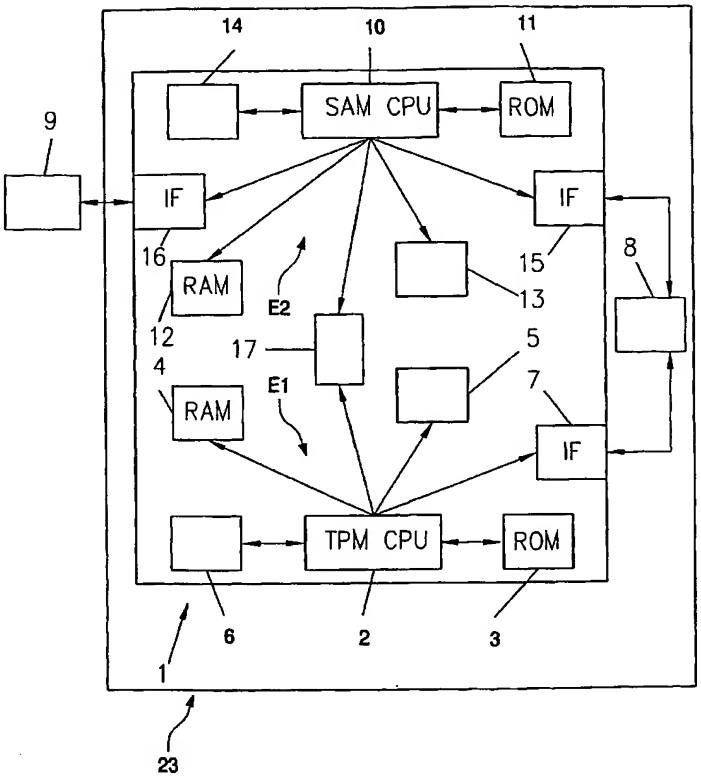
(74) Agent: **RÖGGLA, Harald**; Philips Intellectual Property & Standards, Triester Strasse 64, A-1101 Vienna (AT).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),

[Continued on next page]

(54) Title: METHOD OF AND CIRCUIT FOR IDENTIFYING AND/OR VERIFYING HARDWARE AND/OR SOFTWARE OF AN APPLIANCE AND OF A DATA CARRIER COOPERATING WITH THE APPLIANCE



(57) Abstract: In a method of and circuit for identifying and/or verifying the hardware and/or software of an appliance and of a data carrier, for example a smartcard, cooperating with the appliance, it is provided that a first unit (E1) for verifying the hardware and/or software of the appliance, in particular a Trusted Platform Module (TPM), and a second unit (E2) for verifying and/or identifying and authorizing the external data carrier, in particular a Secure Application Module (SAM), are coupled for direct data exchange via a communication interface (17) of the central arithmetic units (2, 10), in order to reduce or eliminate the possibility of attack or manipulation.

WO 2005/033914 A1

European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:
— *with international search report*